PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-283491
(43)Date of publication of application : 03.10.2003

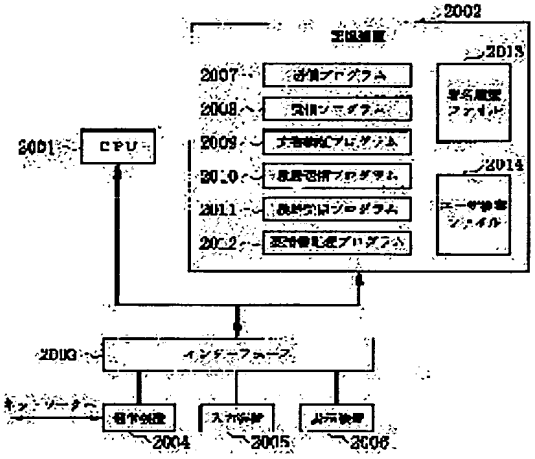
(51)Int.Cl. H04L 9/32
G09C 1/00

(21)Application number : 2002-080392
(22)Date of filing : 22.03.2002

(71)Applicant : HITACHI LTD
(72)Inventor : TANIMOTO KOICHI
ITO SHINJI
MIYAZAKI KUNIHIKO
OMOTO CHIKAHIRO
NISHIOKA KAZUKO

(54) DIGITAL SIGNATURE SYSTEM, DIGITAL SIGNATURE PROCESSOR, PROGRAM AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To efficiently realize a digital signature with high admissibility using a signature history and cross referencing the signature histories by protecting the privacy of the respective users in the case of chained verification.
SOLUTION: Signature numbers (record identification sequential numbers), created signatures and hush values of the previous signature generation records to be used for verification of the chain of the signatures are left as generation records of the respective signatures in a signature history file 2013. In addition, in order to cross reference the signature histories, the signature history file 2013 is updated also in reception of a document with signatures. Furthermore, parties of transmission/reception of the document with signatures are in a user retrieval file 2014 with the signature numbers in the case of updating the signature history file 2013, for the respective signature generation records, to what user they are transmitted or from what user they are received are investigated based on the user retrieval file 2014 in the case of cross referencing the signature histories.



LEGAL STATUS

[Date of request for examination] 11.03.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－283491
（P2003－283491A）
(43)公開日　平成15年10月3日(2003.10.3)

(51)Int.Cl.⁷	識別記号	FI	テーマコード（参考）
H04L 9/32		G09C 1/00	640D 5J104
G09C 1/00	640		640E
		H04L 9/00	675B

審査請求　未請求　請求項の数14　ＯＬ　（全 16 頁）

(21)出願番号　特願2002－80392(P2002－80392)

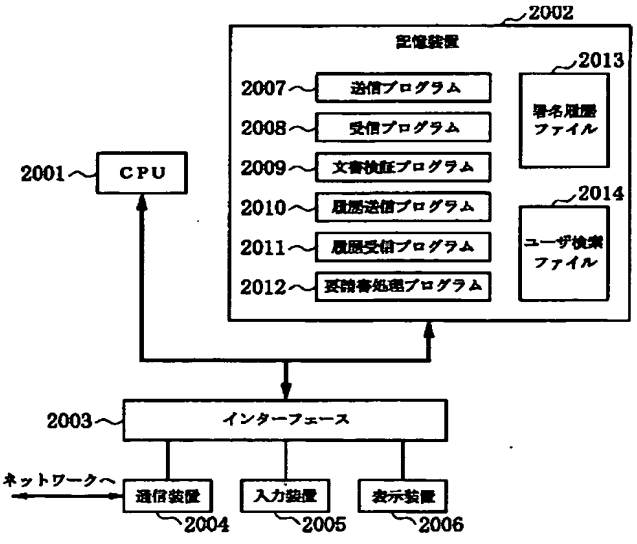
(22)出願日　平成14年３月22日(2002.3.22)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　谷本　幸一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　伊藤　信治
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100077274
弁理士　磯村　雅俊　（外１名）

最終頁に続く

(54)【発明の名称】　ディジタル署名管理方法とディジタル署名処理装置およびプログラムと記録媒体

(57)【要約】
【課題】　連鎖の検証の際の各ユーザのプライバシーを保護して、署名履歴を用いた証拠性の高いディジタル署名、ならびに署名履歴交差を効率的に実現する。
【解決手段】　署名履歴ファイル２０１３中の各署名生成記録として、署名番号（レコード識別用連番）と、作成した署名、および、履歴の連鎖の検証に用いる前回の署名生成記録のハッシュ値を残す。また、署名履歴交差を実現するために、署名付き文書受信時にも署名履歴ファイル２０１３を更新する。さらに、ユーザ検索ファイル２０１４に、署名履歴ファイル２０１３の更新時に、署名付き文書の送受信相手を署名番号とともに保存し、署名履歴交差利用時、ユーザ検索ファイル２０１４に基づき、各署名生成記録について、どのユーザに送信、もしくはどのユーザから受信した署名に対するものであるかを調べる。



【特許請求の範囲】

【請求項１】　送信対象のメッセージに対するディジタル署名の生成に、過去のディジタル署名の生成記録情報を反映させ、生成する全てのディジタル署名に連鎖構造を持たせると共に、受信したメッセージに対する送信元のディジタル署名生成記録情報を生成して署名履歴交差を行うディジタル署名システムにおけるディジタル署名管理方法であって、メッセージとディジタル署名と共に受信した当該ディジタル署名の検証用のデータを用いて、当該メッセージに対する送信元のディジタル署名生成記録情報を生成し、上記過去のディジタル署名の生成記録情報として、記憶装置に記憶された署名履歴ファイルに登録する手順と、上記署名履歴ファイルに登録した各ディジタル署名生成記録情報に対応付けて、当該ディジタル署名生成記録情報が送信時もしくは受信時のいずれの際に生成されたかを示す情報と、当該ディジタル署名生成記録情報の生成元メッセージの送信先もしくは送信元の識別情報とを、記憶装置に記憶されたユーザ検索ファイルに登録する手順と、上記ユーザ検索ファイルに登録された情報に基づき、上記署名履歴ファイルから、署名履歴交差に用いるディジタル署名生成記録情報を特定する手順とを有することを特徴とするディジタル署名管理方法。

【請求項２】　請求項１記載のディジタル署名管理方法であって、送信対象のメッセージあるいはそのハッシュ値と、前回登録したディジタル署名生成記録情報のハッシュ値と、今回登録するディジタル署名生成記録情報の識別情報とを結合したデータに、秘密鍵を作用させて当該メッセージに対するディジタル署名を生成する手順を有することを特徴とするディジタル署名管理方法。

【請求項３】　請求項１、もしくは、請求項２のいずれかに記載のディジタル署名管理方法であって、新たなメッセージの送信に伴い上記署名履歴ファイルにディジタル署名生成記録情報を追加登録する際、追加登録するディジタル署名生成記録情報の識別情報と、上記新たなメッセージの送信に対応して生成したディジタル署名と、上記署名履歴ファイルに前回登録したディジタル署名生成記録情報のハッシュ値とを結合して上記署名履歴ファイルに追加登録するディジタル署名生成記録情報を生成し、該生成したディジタル署名生成記録情報を上記署名履歴ファイルに追加登録する手順を有することを特徴とするディジタル署名管理方法。

【請求項４】　請求項１から請求項３のいずれかに記載のディジタル署名管理方法であって、上記送信対象のメッセージと共に、該メッセージに対して作成したディジタル署名と、該ディジタル署名を含む上記ディジタル署名生成記録情報の識別情報と、上記署名履歴ファイルに前回登録したディジタル署名生成記録情報のハッシュ値とからなる署名データを送信する手順を有することを特徴とするディジタル署名管理方法。

【請求項５】　請求項１から請求項４のいずれかに記載のディジタル署名管理方法であって、新たなメッセージの受信に対応したディジタル署名生成記録情報を上記署名履歴ファイルに追加登録する際、追加登録するディジタル署名生成記録情報の識別情報と、上記署名履歴ファイルに前回登録したディジタル署名生成記録情報のハッシュ値と、上記新たなメッセージと共に送信側で生成され送られてきた該メッセージに対するディジタル署名および該ディジタル署名を含む上記ディジタル署名生成記録情報の識別情報ならびに送信側の署名履歴ファイルにおける前回登録分のディジタル署名生成記録情報のハッシュ値からなる署名データとを結合して、上記署名履歴ファイルに追加登録するディジタル署名生成記録情報を生成し、該生成したディジタル署名生成記録情報を上記署名履歴ファイルに追加登録する手順を有することを特徴とするディジタル署名管理方法。

【請求項６】　請求項５に記載のディジタル署名管理方法であって、受信したメッセージが、該メッセージと共に受信したディジタル署名の生成者から送信されたものであるかを、該ディジタル署名の生成者が当該ディジタル署名の生成に用いた秘密鍵と対の公開鍵を用いて検証する手順と、過去にメッセージと共に生成あるいは受信したディジタル署名の内、検査対象に指定された検査対象ディジタル署名に対応するディジタル署名生成記録情報が、上記署名履歴ファイルに登録されているか否かを検証する手順と、上記署名履歴ファイルに登録されている上記検査対象ディジタル署名に対応するディジタル署名生成記録情報まで、該署名履歴ファイルに登録され正当性が確認されている署名生成記録情報を起点として、連鎖の検証を行う手順とを有することを特徴とするディジタル署名管理方法。

【請求項７】　請求項１から請求項６のいずれかに記載のディジタル署名管理方法であって、上記署名履歴ファイルに登録したディジタル署名生成記録情報を、上記メッセージの送信と同様の手順で送信して上記署名履歴ファイルの更新を行う手順と、送られてきた上記ディジタル署名生成記録情報を、上記メッセージの受信と同様の手順で受信して上記署名履歴ファイルの更新を行う手順とを有することを特徴とするディジタル署名管理方法。

【請求項８】　請求項１から請求項７のいずれかに記載のディジタル署名管理方法であって、検証対象ディジタル署名の連鎖検証に必要なディジタル署名生成記録情報が上記署名履歴ファイルに無い場合、上記ユーザ検索ファイルを検索して、連鎖検証に利用するディジタル署名生成記録情報の送信先を特定し、特定した送信先に、上記利用するディジタル署名生成記録情報の識別情報を通知して当該ディジタル署名生成記録情報の返送を要請する手順と、上記ディジタル署名生成記録情報の返送の要請を受けた場合、上記ユーザ検索ファイルを検索して、要請元の特定と該要請元から過去に受信した各ディジタ

ル署名生成記録情報の識別情報の特定とを行い、該特定した識別情報と上記要請元から通知された上記利用するディジタル署名生成記録情報の識別情報とに基づき、上記署名履歴ファイルに登録した、上記要請元から通知された上記利用するディジタル署名生成記録情報を特定し、該特定した上記利用するディジタル署名生成記録情報の連鎖検証に用いるディジタル署名生成記録情報を選択して、上記利用するディジタル署名生成記録情報と共に要請元に送信する手順とを有することを特徴とするディジタル署名管理方法。

【請求項９】　請求項１から請求項８のいずれかに記載のディジタル署名管理方法であって、メッセージの検証の要望を、調停機関装置に行う際、該調停機関装置に、検証対象のメッセージに関わる署名履歴ファイルを提出する手順を有し、該調停機関装置において、上記署名履歴ファイルを用いて検証を行うことを特徴とするディジタル署名管理方法。

【請求項１０】　請求項９に記載のディジタル署名管理方法であって、メッセージの検証の要望を、上記調停機関装置に行う際、該調停機関装置に、検証対象のメッセージに関わる署名履歴ファイルに加えて、さらにユーザ検索ファイルを提出する手順を有し、上記調停機関装置において、上記署名履歴ファイルと上記ユーザ検索ファイルを用いて検証を行うことを特徴とするディジタル署名管理方法。

【請求項１１】　請求項１から請求項１０のいずれかに記載のディジタル署名管理方法であって、上記署名履歴ファイルに登録した最新のディジタル署名生成記録情報を、公開機関装置に、定期的もしくは定数回毎に送信する手順を有し、該公開機関装置において、受信したディジタル署名生成記録情報を審査して公開することを特徴とするディジタル署名管理方法。

【請求項１２】　送信対象のメッセージに対するディジタル署名の生成に、過去のディジタル署名の生成記録情報を反映させ、生成する全てのディジタル署名に連鎖構造を持たせると共に、受信したメッセージに対する送信元のディジタル署名生成記録情報を生成して署名履歴交差を行うディジタル署名処理装置であって、請求項１から請求項１１のいずれかに記載のディジタル署名管理方法における各手順を実行する各機能を有することを特徴とするディジタル署名処理装置。

【請求項１３】　コンピュータに、請求項１から請求項１１のいずれかに記載のディジタル署名管理方法における各手順を実行させるためのプログラム。

【請求項１４】　コンピュータに、請求項１から請求項１１のいずれかに記載のディジタル署名管理方法における各手順を実行させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタル署名技術に係わり、特に、ディジタル署名の証拠性を高めるのに好適なディジタル署名技術に関するものである。

【０００２】

【従来の技術】ネットワークを介しての電子商取引やオンラインショッピング等においては、そのデータ（メッセージ、文書）が特定の送信者が送信したデータであることを証明し、いわゆる「なりすまし」を防止するために、ディジタル署名（電子署名）技術が利用されている。

【０００３】このディジタル署名（電子署名）では、例えば文書（メッセージ）のハッシュ値で当該文書（メッセージ）の中身を保証し、文書（メッセージ）の改竄を防止できる。

【０００４】また、このようなディジタル署名の証拠性を高める従来技術として、例えば、特開２００１－３３１１０４号公報、および、特開２００１－３３１１０５号公報に記載の技術がある。

【０００５】これらの公知文献には、署名作成の際、その時点までの署名履歴情報を反映させる技術が記載されている。すなわち、この技術では、作成した署名の署名情報を、作成する毎に、新たに署名履歴に追加する。これにより、作成した全ての署名は連鎖構造を持ち、検証の際は、署名に対する検証の他に、連鎖の検証も行うので、改竄は困難となる。

【０００６】上記特開２００１－３３１１０４号公報においては、さらに証拠性を高めるための技術として、「署名履歴交差」技術が記載されている。この「署名履歴交差」技術は、相手から送られてきた署名に対して、署名履歴情報を作成し、これによって相手の署名情報を自分の署名履歴に取り込むというものである。

【０００７】この処理を双方が行うことによって、署名作成時点までの互いの署名履歴が相手の署名履歴に格納され、後に、自分の署名履歴が欠如してしまった場合においても、相手側の署名履歴に残されている自分の署名記録を用いて補うことができる。

【０００８】しかし、これらの公知文献においては、署名履歴にどのような情報を残せば良いのか、また、署名履歴交差は実際にはどのようにやれば良いか、その具体的な実現手法は開示されていない。また、連鎖の検証の際に署名履歴が必要なことから、署名履歴が、自分以外の他人に公開されることがある。

【０００９】

【発明が解決しようとする課題】解決しようとする問題点は、従来の技術では、署名履歴としてどのような情報を残せば良いのか、また、署名履歴交差は実際にはどのようにやれば良いか、その具体的な実現手法が開示されていない点と、署名履歴を利用したディジタル署名においては、連鎖の検証の際に署名履歴が必要なことから、署名履歴が、自分以外の他人に公開されることがある点

である。

【００１０】本発明の目的は、これら従来技術の課題を解決し、各ユーザのプライバシーを保護しながら、なおかつ、署名履歴を用いた証拠性の高いディジタル署名、ならびに署名履歴交差を効率的に実現することである。

【００１１】

【課題を解決するための手段】上記目的を達成するため、本発明では、効率的な署名履歴交差を実現するために、「ユーザ検索ファイル」を新たに用意する。このユーザ検索ファイルには、署名履歴更新時に、署名付き文書の送受信相手を、署名履歴ファイルとの対応付けに用いる各ディジタル署名生成記録情報の識別情報（「署名番号」）とともに保存する。これにより、署名履歴交差利用時には、このユーザ検索ファイルを用いて、各ディジタル署名生成記録情報について、どのユーザに送信、もしくはどのユーザから受信した署名に対するものであるかを調べることができる。

【００１２】尚、署名履歴ファイルに登録する各ディジタル署名生成記録情報は、当該ディジタル署名生成記録情報を特定するための識別情報（「署名番号」）と、「作成したディジタル署名」、および、「前回生成したディジタル署名生成記録情報のハッシュ値」からなり、このディジタル署名生成記録情報は、ディジタル署名が作成されるたびに、そのディジタル署名に対応して生成され、署名履歴ファイルに追加される。「前回生成したディジタル署名生成記録情報のハッシュ値」は、履歴の連鎖を検証するのに用いる。

【００１３】さらに、効率的な署名履歴交差を実現するために、ディジタル署名付き文書の受信時にも署名履歴ファイルを更新する。すなわち、受信したディジタル署名と、ディジタル署名と共に送られてきたデータ（「署名番号」、「前回生成したディジタル署名生成記録情報のハッシュ値」）から、相手のディジタル署名生成記録情報を作成し、「署名番号」、相手の「ディジタル署名生成記録情報のハッシュ値」、および「前回生成したディジタル署名生成記録情報のハッシュ値」をディジタル署名生成記録情報として新たに署名履歴ファイルに追加する。これにより、ディジタル署名付き文書の送信時には、そのディジタル署名に対応した自分のディジタル署名生成記録情報が相手の署名履歴ファイルの中にも保存されることになる。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態を、図面により詳細に説明する。

【００１５】図１は、本発明に係わるディジタル署名システムの構成例を示すブロック図であり、図２は、図１におけるユーザ装置の構成例を示すブロック図、図３は、図２におけるユーザ装置で記憶される署名情報ファイルとユーザ検索ファイルの構成例を示す説明図である。

【００１６】図１におけるディジタル署名システムは、複数のユーザ装置１ａ～１ｃと、公開機関装置２、および、調停機関装置３のそれぞれをネットワーク４を介して接続した構成である。

【００１７】各装置（１ａ～１ｃ，２，３）は、それぞれ、ＣＰＵ（Central Processing Unit）や主メモリ、表示装置、入力装置、外部記憶装置等を有したコンピュータ構成からなり、光ディスク駆動装置等を介してＣＤ－ＲＯＭ等の記憶媒体に記録されたプログラムやデータを外部記憶装置内にインストールした後、この外部記憶装置から主メモリに読み込みＣＰＵで処理することにより、各処理機能を実行している。

【００１８】例えば、ユーザ装置１ａで代表して示す本発明に係わるディジタル署名処理部５における各処理部（送信処理部５ａ、受信処理部５ｂ、文書検証処理部５ｃ、履歴送信処理部５ｄ、履歴受信処理部５ｅ、要請書処理部５ｆ）は、図２に示す各プログラム（２００７～２０１２）のそれぞれに基づくＣＰＵの処理により、各機能が実現される。

【００１９】ユーザ装置１ａ～１ｃは、このディジタル署名処理部５により、本発明に係わるディジタル署名処理装置として、ディジタル署名付き文書を送受信する。また、公開機関装置２は、各ユーザ装置１ａ～１ｃから定期的に送られてくるディジタル署名生成記録情報（以下「署名生成記録」と記載）を審査・公開する。さらに、調停機関装置３は、各ユーザ装置１ａ～１ｃの利用者（ユーザ）間で解決できなかったデータ（メッセージ、文書）の正当性を調査・判定する。

【００２０】ディジタル署名処理装置としてのユーザ装置１ａ～１ｃは、図２に示す構成からなり、本例のディジタル署名システムにおいて、ディジタル署名（以下「署名」と記載）を作成したり、署名付き文書や署名履歴を送受信したり、署名付き文書の検証を行う。

【００２１】図２に示すように、ユーザ装置１ａ～１ｃは、図１におけるディジタル署名処理部５における各機能（送信処理部５ａ、受信処理部５ｂ、文書検証処理部５ｃ、履歴送信処理部５ｄ、履歴受信処理部５ｅ、要請書処理部５ｆ）を実現するための各種プログラム（２００７～２０１２）と署名履歴２０１３とユーザ検索ファイル２０１４が格納されている記憶装置２００２と、ネットワーク４を介して他の装置と通信を行うための通信装置２００４と、キーボードやマウスなどの入力装置２００５と、ディスプレイなどの表示装置２００６と、ＣＰＵ２００１とから構築されている。

【００２２】ＣＰＵ２００１は、インターフェース２００３を介して記憶装置２００２から読み出した各プログラム（送信プログラム２００７、受信プログラム２００８、文書検証プログラム２００９、履歴送信プログラム２０１０、履歴受信プログラム２０１１、要請書処理プログラム２０１２）に基づき、署名の作成や検証、署名

履歴ファイル２０１３の読み込みや更新、ユーザ検索ファイル２０１４の読み込みや更新を行う。

【００２３】本例においては、文書の検証には、「署名のみを使った検証」と、「自分（署名付き文書作成者）の署名履歴を使った検証」、および、「他人の署名履歴を使った検証（署名履歴交差）」とがある。

【００２４】例えば、署名に使用する暗号方式が破られていない場合は、「署名のみを使った検証」で良い。しかしながら、暗号方式が破られた場合や、署名に使った秘密鍵が漏洩した、もしくはその恐れがある場合、また、より確かな検証を行いたい場合は、「自分の署名履歴を使った検証」も行う。さらに、この「自分の署名履歴」が欠如等した場合には、「他人の署名履歴を使った検証」を行う。

【００２５】また、各ユーザ装置１ａ～１ｃは、定期的もしくは定数回毎に最新の署名生成記録を公開機関装置２に送信する。これは、公開機関によって署名生成記録を公開してもらうことにより、その署名生成記録が正当なものであることを示すことを目的とする。

【００２６】公開機関装置２は、各ユーザ装置１ａ～１ｃから受信した署名生成記録の身元を審査し、一般に公開する。公開することにより、正当な署名作成者以外が作成した署名生成記録が不正であることは、正当な署名作成者の指摘により発覚するため、公開した署名生成記録は、正当な署名生成記録であるものとして扱うことができる。

【００２７】尚、公開機関に公開する代わりに、新聞などに公開することによっても、公開した署名生成記録が正当なものであることを示すことができる。

【００２８】調停機関装置３は、各ユーザ装置１ａ～１ｃから文書の正当性の判定の要望があった場合に、検証対象文書に関わる署名履歴ファイル２０１３や、必要に応じて、ユーザ検索ファイル２０１４等を提出させ、それを用いて検証を行い、判定する。

【００２９】例えば、検証に必要な署名履歴が欠如していた場合、署名履歴交差により他人の署名履歴を利用することになるが、個人の要請では協力してもらえないことも想定できる。その場合、調停機関が代わりに協力要請し、署名履歴を取得して、目的の検証を行う。また、各ユーザ装置１ａ～１ｃ間で検証を行った文書について、要望に応じてその結果に対する認定を行う。

【００３０】図２の構成図にあるように、各ユーザ装置１ａ～１ｃでは、送信プログラム２００７、受信プログラム２００８、文書検証プログラム２００９、履歴送信プログラム２０１０、履歴受信プログラム２０１１、要請書プログラム２０１２により、本ディジタル署名システムにおける処理が行われる。

【００３１】また、各ユーザ装置１ａ～１ｃは、署名生成記録を保存するための署名履歴ファイル２０１３と、送受信相手の情報を保存するためのユーザ検索ファイル２０１４とを持ち、それぞれは、図３において示す構成からなる。

【００３２】図３（ａ）に示すように、本例の署名履歴ファイル２０１３は、「番号」、「前回署名記録のハッシュ値」、「文書のハッシュ値」、「署名ｏｒ相手の署名生成記録情報」の各項目３００４～３００７からなるレコード３００１～３００３で構成され、また、図３（ｂ）に示すように、本例のユーザ検索ファイル２０１４は、「番号」、「送受信符号」、「相手情報」の各項目３０１１～３０１３からなるレコード３００８～３０１０で構成されている。

【００３３】署名履歴ファイル２０１３における項目３００４の「番号」は、連番で付与され、署名履歴の中から特定のレコード（「署名生成記録」）を指定するのに用いられる。

【００３４】また、項目３００５の「前回署名記録のハッシュ値」は、履歴の連鎖を検証するのに用いられるものであり、例えば、番号「２」で指定されるレコード３００２における項目３００５の「前回署名記録のハッシュ値」の「Ｈ（Ｓ１）」は、番号「１」で指定されるレコード３００１における各項目３００４～３００７における各値「１」、「Ｈ（Ｓ０）」、「Ｈ（Ｍ１）」、「Ｓｉｇｎ（１||Ｈ（Ｓ０）||Ｈ（Ｍ１））」から算出される。

【００３５】また、項目３００６の「文書のハッシュ値」を署名履歴ファイル２０１３の項目として残すことにより、当該レコード（「署名生成記録」）を改竄するためには、それに対応する署名の作成対象となった文書が必要となり、改竄がより困難となっている。尚、この項目３００６の「文書のハッシュ値」に関しては、署名履歴ファイル２０１３の項目として残すことは必ずしも必要ではない。

【００３６】また、項目３００７の「署名ｏｒ相手の署名生成記録情報」には、自装置での署名生成時には、各項目３００４～３００６に対して生成した署名記録情報が、また、相手方から署名を受信した際には、相手方で同様な手順で生成された署名記録情報が登録される。

【００３７】例えば、レコード３００１は、自装置で生成されたものであり、項目３００７には、項目３００４～３００６の各値（「１」、「Ｈ（Ｓ０）」、「Ｈ（Ｍ１）」）から生成された署名「Ｓｉｇｎ（１||Ｈ（Ｓ０）||Ｈ（Ｍ１））」が記録されている。

【００３８】また、レコード３００２は、相手方装置で生成されたものを受信したものであり、項目３００７には、相手方装置で生成され送られてきた署名データ（「署名番号」、「前回生成した署名生成記録情報のハッシュ値」、「署名」）から生成した値（「３２||Ｈ（Ｓ３２）」）が記録されている。尚、この値「３２||Ｈ（Ｓ３２）」における「３２」は、相手方装置で記録している署名履歴ファイル（２０１３）におけるレコー

ド番号（項目３００４の「番号」の値）である。

【００３９】ユーザ検索ファイル２０１４は、署名履歴交差を効率的に利用するために設けられ、このユーザ検索ファイル２０１４には、署名履歴ファイル２０１３の更新時に、署名付き文書の送受信相手を、「署名番号」とともに保存する。

【００４０】例えば、ユーザ検索ファイル２０１４におけるレコード３００８の項目３０１１の「番号＝１」は、署名履歴ファイル２０１３における項目３００４の「番号＝１」に対応しており、ユーザ検索ファイル２０１４における項目３０１２の「送信」は、署名履歴ファイル２０１３における項目３００４が「番号＝１」のレコード３００１は、自装置で生成されて次の項目３０１３で示される相手方、すなわち「kunihiko@AAA.co.jp」に送信されたことを示している。

【００４１】これにより、署名履歴交差利用時には、このユーザ検索ファイル２０１４を用いて、各署名生成記録について、どのユーザに送信、もしくはどのユーザから受信した署名に対するものであるかを調べることができる。

【００４２】以下、このような構成からなる各ユーザ装置１ａ～１ｃによるディジタル署名システムとしての処理動作を、図４～図９を用いて説明する。

【００４３】図４は、図２におけるユーザ装置の送信プログラムに基づく処理動作例を示すフローチャートであり、図５は、図２におけるユーザ装置の受信プログラムに基づく処理動作例を示すフローチャート、図６は、図２におけるユーザ装置の文書検証プログラムに基づく処理動作例を示すフローチャート、図７は、図２におけるユーザ装置の署名履歴送信プログラムに基づく処理動作例を示すフローチャート、図８は、図２におけるユーザ装置の署名履歴受信プログラムに基づく処理動作例を示すフローチャート、図９は、図２におけるユーザ装置の要請書処理プログラムに基づく処理動作例を示すフローチャートである。

【００４４】本図４に示す例は、図２におけるユーザ装置の送信プログラム２００７に基づく処理動作、すなわち、図１におけるユーザ装置１ａのディジタル処理部５の送信処理部５ａの処理動作例であり、まず、ステップＳ４００１では、署名を作成する対象となる文書に対してハッシュ関数を適用し、文書のハッシュ値を計算する。

【００４５】図３（ａ）に示す署名履歴ファイル２０１３の例では、例えば、レコード３００３（「番号＝３」）における項目３００６の「文書のハッシュ値」として「Ｈ（Ｍ３）」が計算され記録されている。

【００４６】次にステップＳ４００２では、署名履歴ファイル（２０１３）中から、前回署名作成もしくは署名受信時に作成した署名生成記録、すなわち最新の署名生成記録を取り出す。そして、ステップＳ４００３では、ステップＳ４００２で取り出した最新の署名生成記録に対してハッシュ関数を適用し、そのハッシュ値を計算する。

【００４７】例えば、図３（ａ）に示す署名履歴ファイル２０１３におけるレコード３００２が最新の署名生成記録であるとすると、その項目３００７における「署名ｏｒ相手の署名生成記録情報」の「３２||Ｈ（Ｓ３２）」に対してハッシュ関数を適用し、そのハッシュ値を計算し、その結果、レコード３００３における項目３００５の「前回署名記録のハッシュ値」として「Ｈ（Ｓ２）」が記録される。

【００４８】さらにステップＳ４００４では、署名記録番号と、ステップＳ４００１およびステップＳ４００３のそれぞれで得たハッシュ値を結合したデータに対して、秘密鍵を利用してディジタル署名を作成する。

【００４９】ここで、署名記録番号とは、各署名生成記録に固有の（連番で付けられる）番号で、各署名生成記録を判別するのに用いる。例えば、今回作成する署名に対応する署名記録番号は、前回の署名生成記録の記録番号に「１」を加えたものであり、図３（ａ）に示す署名履歴ファイル２０１３の各レコード３００１～３００３における項目３００４の「番号（１～３）」に相当する。

【００５０】そして、このステップＳ４００４でのディジタル署名の作成は、図３（ａ）の例では、例えばレコード３００３で示されるように、署名記録番号「３」と、ステップＳ４００１で得たハッシュ値（「Ｈ（Ｍ３）」）およびステップＳ４００３で得たハッシュ値（「Ｈ（Ｓ２）」）を結合したデータに対して、秘密鍵を利用してディジタル署名（「Ｓｉｇｎ（３||Ｈ（Ｓ２）||Ｈ（Ｍ３））」）が作成される。

【００５１】尚、この署名記録番号（例えば「３」）は必ずしも署名対象データに加える必要はないが、改竄されると署名履歴交差利用に支障をきたすため、これも含めて署名対象データとするのが望ましい。

【００５２】このように、ステップＳ４００４の処理において、ステップＳ４００３で得た前回の署名生成記録のハッシュ値を署名対象データに加えることで、署名対象文書に対して署名履歴を反映させたディジタル署名を生成することができる。

【００５３】次のステップＳ４００５では、前述のステップＳ４００４で署名を作成するのに用いたデータ（署名記録番号、前回署名生成記録のハッシュ値、文書のハッシュ値）と、作成した署名とを結合して署名生成記録を生成する。これが今回作成した署名に対応した署名生成記録となり、図３（ａ）の署名履歴ファイル２０１３の各レコード３００１，３００３（レコード３００２は除く）で例示する構成で記録、管理される。

【００５４】さらに続いてステップＳ４００６において、ユーザ検索ファイル（２０１４）に、今回作成した

署名に対応する署名記録番号と送信先相手の情報を追加する。尚、送信先相手の情報には、例えば、図３（ｂ）のユーザ検索ファイル２０１４の項目３０１３において例示するように、メールアドレスが挙げられる。

【００５５】そして、ステップＳ４００７では、当該文書に、ステップＳ４００４で作成した署名と、検証に必要なデータ（署名記録番号、前回署名生成記録のハッシュ値）、検証に必要な公開鍵および公開鍵証明書を付けて送信する。

【００５６】次に、図５により、図２におけるユーザ装置の受信プログラム２００８に基づく処理動作、すなわち、図１におけるユーザ装置１ａのディジタル処理部５の受信処理部５ｂの処理動作例を説明する。

【００５７】まずステップＳ５００１において、ディジタル署名付き文書を受信した場合には、ステップＳ５００３以下の処理を行う。

【００５８】ステップＳ５００３では、文書とともに送られてきた公開鍵と公開鍵証明書について、正しいものであるか検証を行う。次のステップＳ５００５では、送られてきた文書に対してハッシュ関数を適用してハッシュ値を計算する。

【００５９】ステップＳ５００６では、文書とともに送られてきた署名記録番号、前回署名生成記録のハッシュ値と、ステップＳ５００５で作成した文書のハッシュ値、公開鍵を利用して署名の検証を行う。

【００６０】検証成功であれば、ステップＳ５００８において、署名生成記録を作成し、署名履歴を更新する。例えば、図３（ａ）の署名履歴ファイル２０１３におけるレコード３００２（「番号＝２」）に示すようにして新たなレコードを追加する。

【００６１】この受信時のレコード３００２での署名生成記録は、送信の時とは異なり、文書とともに送られてきたデータから送信元の署名生成記録を作成し、送信時での署名の代わりに、それのハッシュ値（「Ｈ（Ｓ３２）」）を保存する。

【００６２】このように、受信時にも相手の署名情報を記録した署名生成記録を作成して履歴（署名履歴ファイル２０１３）を更新することで、ユーザ間で互いの履歴情報を分散確保するという署名履歴交差を実現し、署名履歴消失などが起こった場合にも、署名履歴交差を利用して対処可能となる。尚、受信時に履歴を更新するかどうかは受信側に毎回選択させても良い。

【００６３】ステップＳ５００９では、ユーザ検索ファイル（２０１４）に、今回受信した署名に対応する署名記録番号と送信元相手の情報を追加する。すなわち、図３（ｂ）のユーザ検索ファイル２０１４のレコード３００９で示すように、その項目３０１２の「送受信符号」は「受信」として記録され、項目３０１３の「相手情報」として、送信元のメールアドレス「s-ito@BBB.co.jp」が記録される。

【００６４】そして最後に、ステップＳ５０１０において、署名付き文書を任意の場所に格納する。

【００６５】次に、図６により、図２におけるユーザ装置の文書検証プログラム２００９に基づく処理動作、すなわち、図１におけるユーザ装置１ａのディジタル処理部５の文書検証処理部５ｃの処理動作例を説明する。

【００６６】この文書検証プログラム２００９は、過去に作成もしくは受信した文書について、署名履歴を利用した署名検証を行うものであり、まずステップＳ６００１，Ｓ６００２において、文書とそれに付けられた署名および検証に必要なデータを利用して、通常の署名検証（図５におけるステップＳ５００３～ステップＳ５００６）を行う。

【００６７】次にステップＳ６００３，Ｓ６００４において、検証対象署名に対応する署名生成記録が、署名履歴中に存在するかどうか、また公開した署名生成記録が署名履歴中に存在するかどうか調べる。ここで使用する署名履歴は、自分の署名履歴ファイル（２０１３）であるか、または、検証対象署名の署名者の署名履歴であるかのどちらかである。

【００６８】署名生成記録の存在を調べる処理は、過去に生成あるいは受信した文書とそのディジタル署名の内、検証対象に指定されたディジタル署名（検証対象ディジタル署名）と、その検証対象ディジタル署名を生成した時あるいは受信した時に作成して署名履歴ファイル（２０１３）に登録された署名生成記録情報中に含まれる署名データ（ディジタル署名と、このディジタル署名を含む署名生成記録情報の番号（識別情報）ならびに前回登録分のディジタル署名生成記録情報のハッシュ値からなる）とが一致しているか照合することで行う。

【００６９】さらに、ステップＳ６００５，６００６において、公開した署名生成記録と履歴中同じ番号の署名生成記録とを比較して、一致するかどうか調べ、ステップＳ６００７，６００８において、検証対象署名と、それに対応する署名生成記録中に保存されている署名とが一致するかどうか調べる。

【００７０】そして、ステップＳ６００９～６０１１では、公開した署名生成記録と同じ番号の署名生成記録を起点として、検証対象署名に対応する署名生成記録まで連鎖を遡って検証する。具体的には、１つ前の署名生成記録のハッシュ値をとったものと、署名生成記録中に残されている前回署名生成記録のハッシュ値との比較を行い、一致すれば２つの署名生成履歴は正しく連鎖が繋がっているものとする。

【００７１】最後に、ステップＳ６０１１において、検証結果を表示する。

【００７２】次に、図７により、図２におけるユーザ装置の署名履歴送信プログラム２０１０に基づく処理動作、すなわち、図１におけるユーザ装置１ａのディジタル処理部５の署名履歴送信処理部５ｄによる署名例歴を

送信する履歴送信ステップ処理動作例を説明する。まずステップＳ７００１において、送信する署名履歴を署名履歴ファイル（２０１３）から取得する。

【００７３】そして、ステップＳ７００２～ステップＳ７００６において、文書送信の時と同様に、署名履歴に対して署名を作成し、署名履歴ファイル（２０１３）、ユーザ検索ファイル（２０１４）を更新する。

【００７４】最後に、ステップＳ７００７において、ステップＳ７００１で取得した署名履歴を相手に送信する。ここで、署名者が過去に署名を付けて送信した文書に対して、受信者が受け取った署名付き文書の正当性を文書検証処理によって検証したい場合には、署名者は、受信者の要請に応じて、検証に必要な署名履歴を署名履歴送信プログラム２０１０に基づき送信する。

【００７５】次に、図８により、図２におけるユーザ装置の署名履歴受信プログラム２０１１に基づく処理動作、すなわち、図１におけるユーザ装置１ａのディジタル処理部５の署名履歴受信処理部５ｅによる署名履歴を受信する履歴受信ステップの処理動作例を説明する。

【００７６】この署名履歴受信プログラム２０１１に基づきユーザ装置は、ステップＳ８００１～ステップＳ８００８において、受け取った署名履歴とそれに付けられた署名について、通常の署名検証を行い、署名履歴ファイル（２０１３）、ユーザ検索ファイル（２０１４）の更新を行う。

【００７７】そして、ステップＳ８００９において、受信した署名履歴をハードディスク等の記憶装置に格納する。格納した署名履歴は、文書検証処理の際に利用される。

【００７８】次に、図９により、図２におけるユーザ装置の要請書処理プログラム２０１２に基づく処理動作、すなわち、図１におけるユーザ装置１ａのディジタル処理部５の要請書処理部５ｆの処理動作例を説明する。この要請書処理プログラム２０１２は、署名履歴交差を利用する際に使用する要請書を扱うものである。

【００７９】この署名履歴交差は、検証したい署名に対応する署名生成記録以後に公開した署名生成記録が無い場合や、履歴の一部が欠如して連鎖が検証できない場合などに、相手の署名生成記録を利用して検証可能にする技術である。また、要請書は、署名履歴交差を利用した検証に必要な署名生成記録を相手に要請するために使用する文書である。

【００８０】署名履歴交差を利用する際には、誰に要請書を送ればよいか決定しなければならない。すなわち、目的の署名の検証を行うためには、自分の署名履歴中どの署名生成記録の正当性が証明できれば良いか調べた後に、その署名生成記録が誰の署名履歴に保存されているかを知らなければならない。

【００８１】このように、各署名生成記録がどの署名に対応しているか、すなわち誰に送信した文書に付けた署名に対応しているか、あるいは誰から受信した署名についてのものであるかを知る技術として、取引相手の情報（例えば、メールアドレス）も署名生成記録に残しておくことが有効である。

【００８２】しかしながら、署名履歴は、文書検証を行う際や、署名履歴交差を利用する際に、その一部もしくは全てを他人に渡すため、取引相手の情報が署名生成記録に残っていた場合、それによって誰と取引しているか他人に漏洩してしまう。

【００８３】本例では、取引相手の情報を、署名履歴（２０１３）とは別のユーザ検索ファイル（２０１４）に保存し、各署名生成記録とユーザ検索ファイル（２０１４）中の取引相手情報とは、署名記録番号によってのみ対応付けているため、署名履歴を公開もしくは他人に送信した場合であっても、取引相手の情報が漏洩することはない。

【００８４】すなわち、ユーザ装置は、要請書処理プログラム２０１２に基づき、まずステップＳ９００１，Ｓ９００２において、要請書処理内容が要請書の受信であるか送信であるか判別し、送信であれば、ステップＳ９００３において、検証対象署名の検証が可能となるためにはどの署名生成記録の正当性が証明できれば良いか検索する。

【００８５】このステップＳ９００３で検索した検証に必要な署名生成記録について、ステップＳ９００４において、その署名記録番号を参照して、ユーザ検索ファイル（２０１４）から、検証に必要な署名生成記録が誰のところに保存されているか調べる。

【００８６】そして、ステップＳ９００５において、ステップＳ９００４で検索したユーザに対して、必要な署名生成記録の番号を記した要請書を送信する。

【００８７】また、ステップＳ９００２の判別結果が、要請書の受信であれば、まず要請書送信元の情報（例えば、メールアドレス）に基づき、ステップＳ９００６において、ユーザ検索ファイル（２０１４）を検索して、以前に要請書送信元ユーザから文書を受信した際に生成した署名生成記録を探す。

【００８８】次に、ステップＳ９００７において、ステップＳ９００６で検索した署名生成記録の中から、要請書に記載されている署名記録番号（相手が必要とする署名生成記録の番号）に該当する相手の署名生成記録が保存されている署名生成記録を抽出する。

【００８９】そして、ステップＳ９００８において、要請書送信元が目的の署名を検証するために必要な署名生成記録を求める。具体的には、ステップＳ９００７で抽出した署名生成記録以後に公開した署名生成記録を見つけ、ステップＳ９００７で抽出した署名生成記録から、公開した署名生成記録までの全ての署名生成記録を、相手が検証に必要な署名生成記録とする。

【００９０】最後に、ステップＳ９００９において、ス

テップＳ９００８で求めた署名生成記録を要請書送信元へ送信する。

【００９１】このような、要請書送信者と要請書受信者が署名履歴交差を利用する際の手順について、図１０を用いて、より具体的に説明する。

【００９２】図１０は、本発明に係わるディジタル署名システムの処理動作の具体例を示す説明図である。

【００９３】本図１０における例では、ユーザ装置Ａは、Ａの署名履歴１０００１中、署名記録番号「２７」に対応する署名を検証したいが、署名生成記録番号「３１」以降の履歴が欠如してしまい、このままでは署名を検証することができない。しかしながら、本例によれば、以下のように署名履歴交差を利用することにより、署名の検証が可能となる。

【００９４】ユーザ装置Ａは、署名記録番号「２７～３１」の間で、ユーザ装置Ａの署名生成記録が保存されている可能性のある相手を、Ａのユーザ検索ファイル１０００２を用いて検索する。

【００９５】その結果、例えば、記録番号「３０」の署名生成記録は、ユーザ装置Ｂに署名付き文書を送信する際に生成した署名の署名生成記録であるから、ユーザ装置Ｂの署名履歴にはユーザ装置Ａの「３０」番の署名生成記録が保管されていることが分かる（図中「（１）」）。

【００９６】そこで、ユーザ装置Ａは、署名記録番号「３０」の署名生成記録が必要であるという内容の要請書１０００３を作成し、ユーザ装置Ｂに送信する（図中「（２）」）。

【００９７】このように、本例では、要請書の送受信によって、検証に必要な署名履歴を相手に伝え、協力を要請する。これにより署名履歴交差を利用した検証を実現する。

【００９８】すなわち、要請者ユーザ装置Ａから要請書１０００３を受け取ったユーザ装置Ｂは、Ｂのユーザ検索ファイル１０００４を用いて、Ｂの署名履歴１０００５中、ユーザ装置Ａから署名付き文書を受信した時に生成した署名生成記録を検索する。その結果、例えば、Ｂの署名履歴１０００５中、署名記録番号「２１」と「２３」の署名生成記録が該当署名記録であることがわかる（図中「（３）」）。

【００９９】ユーザ装置Ｂでは、Ｂの署名履歴１０００５中、記録番号「２１」と「２３」の署名生成記録を調べることにより、例えば、ユーザ装置Ａが必要とするユーザ装置Ａの「３０」番の署名生成記録を保存している署名生成記録は、「２１」番の署名生成記録であると特定できる。

【０１００】本図１０において、Ｂの署名履歴１０００５中の「２４」番の署名生成記録は、図１における公開機関装置２で公開しているので、「２１」～「２４」番の署名生成記録をユーザ装置Ｂからユーザ装置Ａに送信すれば、ユーザ装置Ａは、ユーザ装置Ｂから送られてきた署名履歴を用いて目的の署名を検証することができる。そこで、ユーザ装置Ｂは、「２１」～「２４」番の署名生成記録をユーザ装置Ａに送信する（図中「（４）」）。

【０１０１】ユーザ装置Ａは、ユーザ装置Ｂから送られてきた「２１」～「２４」番の署名生成記録を用いて目的の署名（「２７」）を検証する。

【０１０２】以上、図１～図１０を用いて説明したように、本例では、署名履歴ファイル２０１３中の各署名生成記録（ディジタル署名生成記録情報）には、署名番号（識別情報）と、作成した署名（ディジタル署名）、および、前回の署名生成記録のハッシュ値を残す。ここで署名生成記録（ディジタル署名生成記録情報）とは、履歴（署名履歴ファイル２０１３）に残すために各署名（ディジタル署名）作成時に生成する署名情報であり、署名（ディジタル署名）が作成されるたびに、その署名に対応した署名生成記録が生成され、履歴（署名履歴ファイル２０１３）に追加される。また、「署名番号」（識別情報）は、連番で付加し、署名履歴の中から特定の署名生成記録（ディジタル署名生成記録情報）を指定するのに用いる。また、作成した署名（ディジタル署名）は、署名生成記録（ディジタル署名生成記録情報）とそれに対応する署名との関係が正しいことを証明する。そして、前回の署名生成記録のハッシュ値は、履歴の連鎖を検証するのに用いる。

【０１０３】さらに、本例では、署名履歴交差を実現するために、署名付き文書受信時にも署名履歴ファイル２０１３を更新する。すなわち、署名とともに送られてきたデータから、相手の署名生成記録（ディジタル署名生成記録情報）を作成し、署名番号（識別情報）、相手の署名生成記録（ディジタル署名生成記録情報）のハッシュ値、前回の署名生成記録（ディジタル署名生成記録情報）のハッシュ値を、今回の署名生成記録（ディジタル署名生成記録情報）として新たに履歴（署名履歴ファイル２０１３）に追加する。これにより、署名付き文書の送信時には、その署名（ディジタル署名）に対応した自分の署名生成記録（ディジタル署名生成記録情報）が相手の署名履歴（署名履歴ファイル２０１３）の中にも保存されることになる。

【０１０４】そして、より効率的な署名履歴交差を実現するために、ユーザ検索ファイル２０１４を新たに用意する。このユーザ検索ファイル２０１４には、署名履歴（署名履歴ファイル２０１３）の更新時に、ディジタル署名付きデータ（メッセージ、文書）の送受信相手を、署名番号（識別情報）とともに保存する。これにより、署名履歴交差の利用時には、ユーザ検索ファイル２０１４を用いて、各署名生成記録（ディジタル署名生成記録情報）について、どのユーザに送信、もしくはどのユーザから受信した署名に対するものであるかを調べること

ができる。

【０１０５】すなわち、本例では、ディジタル署名生成側のユーザ装置において、メッセージあるいはそのハッシュ値に、ディジタル署名生成者が有する秘密鍵を作用させ、当該メッセージに対するディジタル署名を生成する署名生成処理と、生成したディジタル署名から、その署名情報を記録した署名生成記録（ディジタル署名生成記録情報）を生成し、過去に生成された署名生成記録が登録されている署名履歴（署名履歴ファイル２０１３）に新たに生成した署名生成記録を追加する署名履歴更新処理と、生成したディジタル署名とメッセージを含むディジタル署名付きメッセージを送信する送信処理とを行い、また、ディジタル署名検証者側のユーザ装置において、送付されたディジタル署名付きメッセージを、検証対象ディジタル署名付きメッセージとして受け付ける受信処理と、受信したディジタル署名付きメッセージが、ディジタル署名生成者により送付されたものであるかを、秘密鍵と対の公開鍵を用いてメッセージとディジタル署名が正しく対応しているかを調べることにより検証する検証処理と、受信したディジタル署名から、その署名情報を記録した署名生成記録を生成し、過去に生成された署名生成記録が登録されている署名履歴（署名履歴ファイル２０１３）に新たに生成した署名生成記録を追加する署名履歴更新処理とを行う。

【０１０６】また、ディジタル署名生成側での署名生成処理は、メッセージあるいはそのハッシュ値と、前回署名作成時あるいは受信時に記録された署名生成記録のハッシュ値と、作成した署名生成記録の中から特定の署名生成記録を識別するために署名生成記録ごとに付けられた署名記録番号（識別情報）とを結合した署名対象データに、秘密鍵を作用させて、当該メッセージに対するディジタル署名を生成する。

【０１０７】また、ディジタル署名生成側での署名履歴更新処理は、作成した署名生成記録の中から特定の署名生成記録を識別するために署名生成記録ごとに付けられた署名記録番号（識別情報）と、作成した署名と、前回署名作成時あるいは受信時に生成した署名生成記録のハッシュ値とを結合して、今回生成した署名に対する署名生成記録を作成し、過去に生成された署名生成記録が登録されている署名履歴（署名履歴ファイル２０１３）に、今回、新たに生成した署名生成記録を追加する。

【０１０８】また、履歴更新処理では、署名履歴の更新に加えて、各署名付きメッセージの取引相手を記録するために、署名生成時あるいは署名付きメッセージ受信時に、その時生成あるいは受信した署名情報が記録された署名生成記録に固有の署名記録番号（識別情報）と、生成した署名の送信相手あるいは受信した署名の作成者（送信元）のユーザ情報とを記録したユーザ検索ファイル（２０１４）を更新する。

【０１０９】また、ディジタル署名生成側の送信処理では、メッセージと、それに対して作成されたディジタル署名と、ディジタル署名に対して作成した署名生成記録の署名記録番号（識別情報）と、前回署名作成時あるいは受信時に記録された署名生成記録のハッシュ値とを送信する。

【０１１０】また、ディジタル署名検証側の署名履歴更新処理では、ディジタル署名側より送られてきた署名データと、作成した署名生成記録の中から特定の署名生成記録を識別するために署名生成記録ごとに付けられた署名記録番号（識別情報）と、前回署名作成時あるいは受信時に作成した署名生成記録のハッシュ値とを結合して、今回受信した署名に対する署名生成記録を作成し、過去に生成された署名生成記録が登録されている署名履歴（署名履歴ファイル２０１３）に、新たに今回作成した署名生成記録を追加する。

【０１１１】また、ディジタル署名検証側の検証処理に加えて、過去に生成あるいは受信した検証対象ディジタル署名に対して、その過去に生成あるいは受信した検証対象ディジタル署名と、そのディジタル署名を生成した時あるいは受信した時に作成した署名生成記録中に含まれる署名データとが一致しているか検証し、さらに、最新の正当な署名生成記録から検証対象ディジタル署名データが含まれる署名生成記録まで署名生成記録の連鎖が正しく繋がっているかを検証する履歴検証処理を行う。

【０１１２】さらに、署名履歴を送信する履歴送信処理、または、署名履歴を受信する履歴受信処理を行う。

【０１１３】また、ディジタル署名検証者側の装置では、署名履歴を用いた検証を行う際、検証に必要な署名履歴が無い場合、他のユーザの署名履歴を利用するために、検証に必要な署名生成記録の署名記録番号を他のユーザに伝える要請書送信処理を行う。

【０１１４】また、要請書受信した際、要請書受信側は、要請書記載の要求署名記録に応じて、要請書送信側に、署名履歴の全部もしくは一部を送信する要請書受信処理を行う。

【０１１５】このような要請書送信先の決定や、履歴送信において送信する履歴の範囲を決定する時には、ユーザ検索ファイル２０１４に記録された署名記録番号と送受信相手の情報を利用する。

【０１１６】このように、本例では、署名履歴を利用した、ディジタル署名の改竄・偽造がより困難であるディジタル署名技術を提供することができ、また、他人の履歴を用いた検証や、署名生成記録の分散確保により、自分の署名履歴が欠如した場合でも、他人の署名履歴を利用して、欠如を補って検証することができ、より安全性と信頼性の高いディジタル署名技術を実現することができる。

【０１１７】尚、本発明は、図１～図１０を用いて説明した例に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能である。例えば、本例で

は、図１に示すように、各ユーザ装置１ａ～１ｃと公開機関装置２、調停機関装置３のそれぞれをネットワークを介して接続した構成としているが、調停機関装置３を用いない構成としても良く、また、新聞等での公開を行うことで、公開機関装置２も用いない構成、すなわち、各ユーザ装置１ａ～１ｃからなる構成としても良い。

【０１１８】また、各ユーザ装置１ａ～１ｃに関しても、この３台の構成に限るものではなく、より多くのユーザ装置を設けることでも良い。また、このユーザ装置１ａ～１ｃの構成に関しても、図２に示される構成に限るものではなく、例えば、マイクや音声変換機能等を設けて、音声データを対象としてディジタル署名を施す構成としても良い。

【０１１９】また、本例では、光ディスクをプログラムの記録媒体として用いているが、ＦＤ（Flexible Disk）等を記録媒体として用いることでも良い。また、プログラムのインストールに関しても、通信装置を介してネットワーク経由でプログラムをダウンロードしてインストールすることでも良い。

【０１２０】

【発明の効果】本発明によれば、連鎖の検証の際にも、署名履歴が、自分以外の他人に公開されることがなく、各ユーザのプライバシーを保護しながら、なおかつ、署名履歴を用いた証拠性の高いディジタル署名、ならびに署名履歴交差を効率的に実現することが可能である。

【図面の簡単な説明】

【図１】本発明に係わるディジタル署名システムの構成例を示すブロック図である。

【図２】図１におけるユーザ装置の構成例を示すブロック図である。

【図３】図２におけるユーザ装置で記憶される署名情報ファイルとユーザ検索ファイルの構成例を示す説明図である。

【図４】図２におけるユーザ装置の送信プログラムに基づく処理動作例を示すフローチャートである。

【図５】図２におけるユーザ装置の受信プログラムに基づく処理動作例を示すフローチャートである。

【図６】図２におけるユーザ装置の文書検証プログラムに基づく処理動作例を示すフローチャートである。

【図７】図２におけるユーザ装置の署名履歴送信プログラムに基づく処理動作例を示すフローチャートである。

【図８】図２におけるユーザ装置の署名履歴受信プログラムに基づく処理動作例を示すフローチャートである。

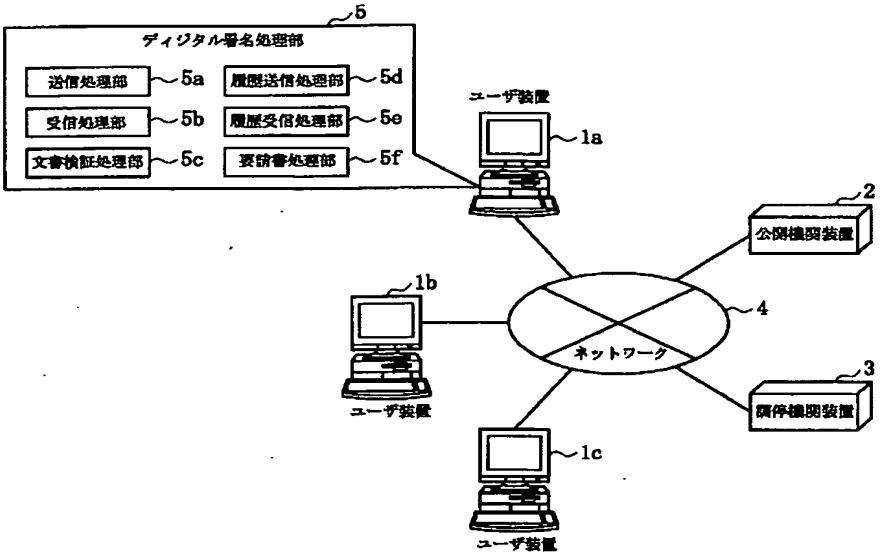
【図９】図２におけるユーザ装置の要請書処理プログラムに基づく処理動作例を示すフローチャートである。

【図１０】本発明に係わるディジタル署名システムの処理動作の具体例を示す説明図である。

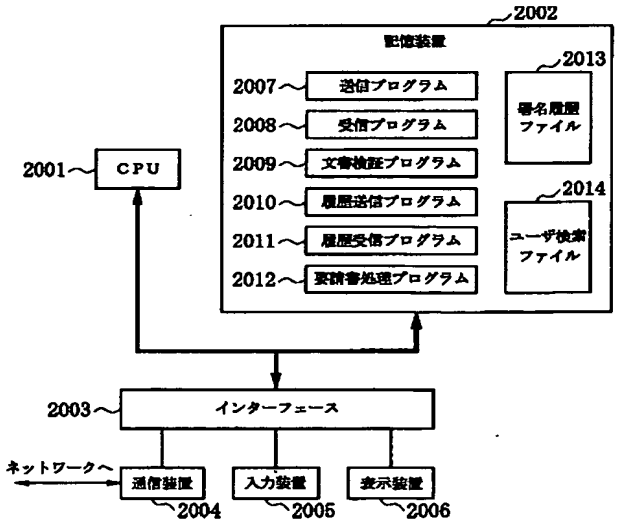
【符号の説明】

１ａ～１ｃ：ユーザ装置、２：公開機関装置、３：調停機関装置、４：ネットワーク、２００１：ＣＰＵ、２００２：記憶装置、２００３：インターフェース、２００４：通信装置、２００５：入力装置、２００６：表示装置、２００７：送信プログラム、２００８：受信プログラム、２００９：文書検証プログラム、２０１０：履歴送信プログラム、２０１１：履歴受信プログラム、２０１２：要請書処理プログラム、２０１３：署名履歴ファイル、２０１４：ユーザ検索ファイル、３００１～３００３：レコード、３００４：項目（「番号」）、３００５：項目（「前回署名記録のハッシュ値」）、３００６：項目（「文書のハッシュ値」）、３００７：項目（「署名または相手の署名生成記録情報」）、３００８～３０１０：レコード、３０１１：項目（「番号」）、３０１２：項目（「送受信符号」）、３０１３：項目（「相手情報」）、１０００１：ユーザ装置Ａの署名履歴、１０００２：ユーザ装置Ａのユーザ検索ファイル、１０００３：要請書、１０００４：ユーザ装置Ｂのユーザ検索ファイル、１０００５：ユーザ装置Ｂの署名履歴。

【図１】



【図２】



【図３】

(a)

署名履歴ファイル　2013

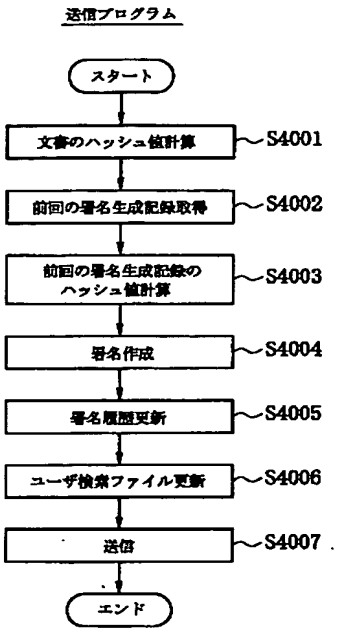
	3004 番号	3005 前回署名記録のハッシュ値	3006 文書のハッシュ値	3007 署名or相手の署名生成記録情報
3001	1	$H(S_0)$	$H(M_1)$	$Sign(1 \| H(S_0) \| H(M_1))$
3002	2	$H(S_1)$	—	$32 \| H(S_{22})$
3003	3	$H(S_2)$	$H(M_3)$	$Sign(3 \| H(S_2) \| H(M_3))$

(b)

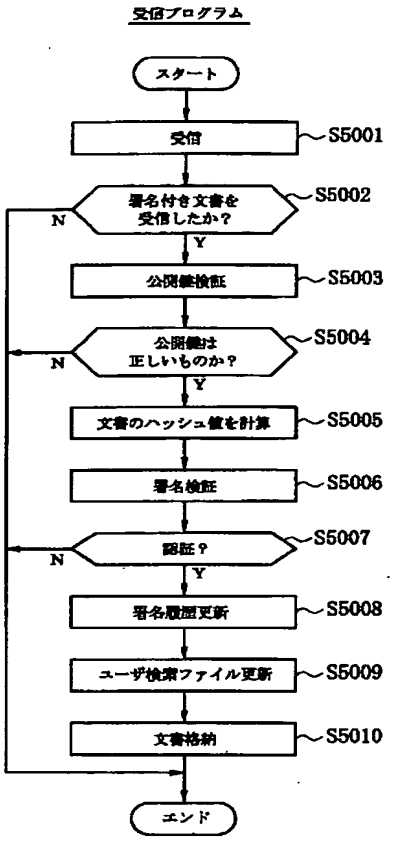
ユーザ検索ファイル　2014

	3011 番号	3012 送受信符号	3013 相手情報
3008	1	送信	kunihiko@AAA.co.jp
3009	2	受信	s-itoh@BBB.co.jp
3010	3	送信	tamamoto@CCC.co.jp

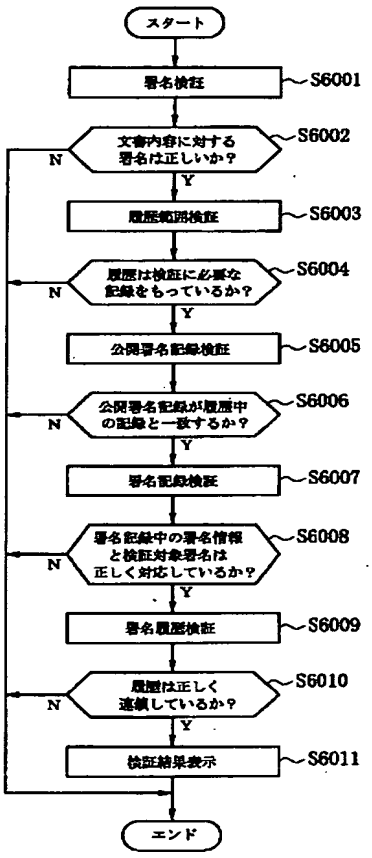
【図４】


送信プログラム
スタート
文書のハッシュ値計算
S4001
前回の署名生成記録取得
S4002
前回の署名生成記録の
ハッシュ値計算
S4003
署名作成
S4004
署名履歴更新
S4005
ユーザ検索ファイル更新
S4006
送信
S4007
エンド

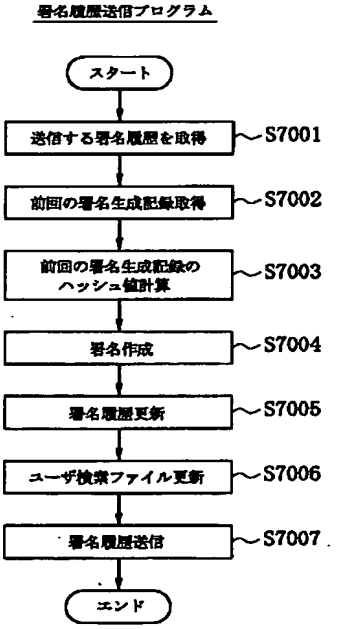
【図５】


受信プログラム
スタート
受信
S5001
署名付き文書を
受信したか？
S5002
N
Y
公開鍵検証
S5003
公開鍵は
正しいものか？
S5004
N
Y
文書のハッシュ値を計算
S5005
署名検証
S5006
認証？
S5007
N
Y
署名履歴更新
S5008
ユーザ検索ファイル更新
S5009
文書格納
S5010
エンド

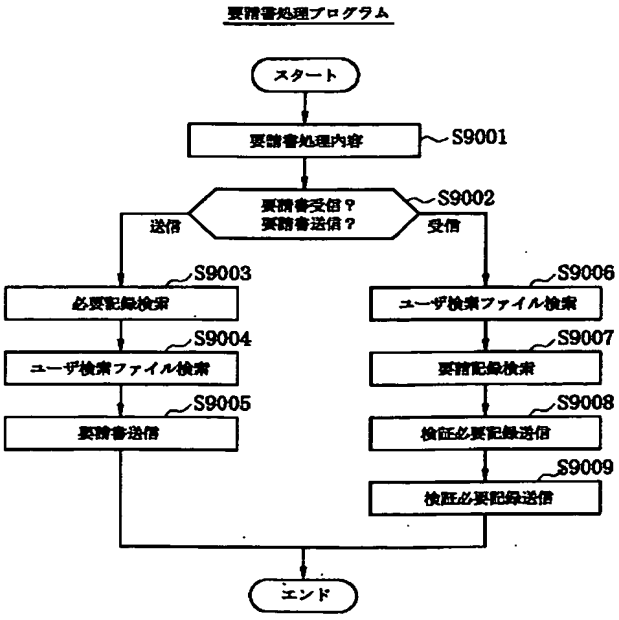
【図６】


文書検証プログラム
スタート
署名検証
S6001
文書内容に対する
署名は正しいか？
S6002
N
Y
履歴範囲検証
S6003
履歴は検証に必要な
記録をもっているか？
S6004
N
Y
公開署名記録検証
S6005
公開署名記録が履歴中
の記録と一致するか？
S6006
N
Y
署名記録検証
S6007
署名記録中の署名情報
と検証対象署名は
正しく対応しているか？
S6008
N
Y
署名履歴検証
S6009
履歴は正しく
連続しているか？
S6010
N
Y
検証結果表示
S6011
エンド

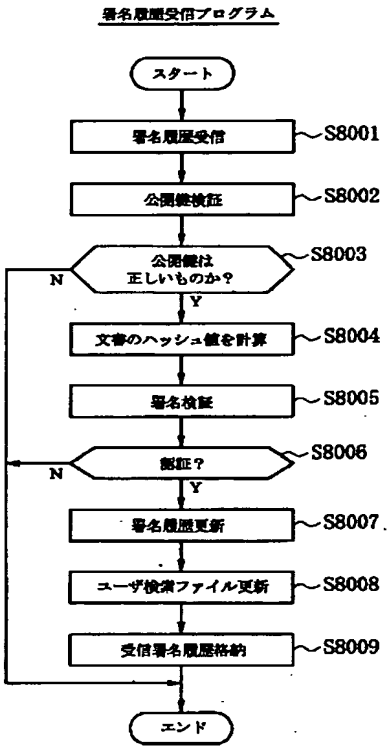
【図７】


署名履歴送信プログラム
スタート
送信する署名履歴を取得
S7001
前回の署名生成記録取得
S7002
前回の署名生成記録の
ハッシュ値計算
S7003
署名作成
S7004
署名履歴更新
S7005
ユーザ検索ファイル更新
S7006
署名履歴送信
S7007
エンド

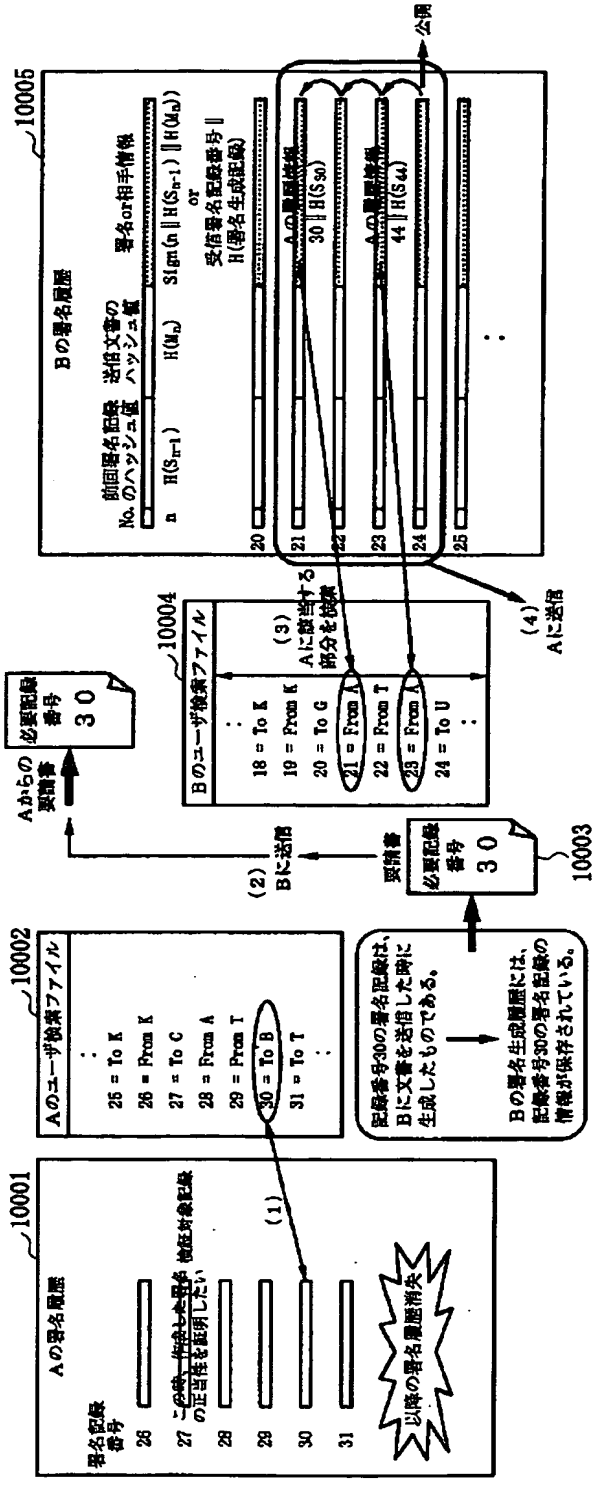
【図９】


要請書処理プログラム
スタート
要請書処理内容
S9001
要請書受信？
要請書送信？
S9002
送信
受信
必要記録検索
S9003
ユーザ検索ファイル検索
S9004
要請書送信
S9005
ユーザ検索ファイル検索
S9006
要請記録検索
S9007
検証必要記録送信
S9008
検証必要記録送信
S9009
エンド

【図８】


署名履歴受信プログラム
スタート
署名履歴受信
S8001
公開鍵検証
S8002
公開鍵は
正しいものか？
S8003
N
Y
文書のハッシュ値を計算
S8004
署名検証
S8005
認証？
S8006
N
Y
署名履歴更新
S8007
ユーザ検索ファイル更新
S8008
受信署名履歴格納
S8009
エンド

【図１０】


10001
Aの署名履歴
署名記録番号
26
27
28
29
30
31
(1)
以降の署名履歴消失
10002
Aのユーザ検索ファイル
25 = To K
26 = From K
27 = To C
28 = From A
29 = From T
30 = To B
31 = To T
10003
要請書
必要記録番号 30
(2) Bに送信
Aからの要請書
必要記録番号 30
10004
Bのユーザ検索ファイル
(3) Aに該当する部分を検索
18 = To K
19 = From K
20 = To G
21 = From A
22 = From T
23 = From A
24 = To U
10005
Bの署名履歴
前回署名記録No.のハッシュ値
送信文書のハッシュ値
署名or相手情報
n
H(S_{n-1})
H(M_n)
Sig_n(n ‖ H(S_{n-1}) ‖ H(M_n))
or
受信署名記録番号 ‖ H(署名生成記録)
20
21
22
23
24
25
公開
(4) Aに送信
Bの署名生成履歴には、記録番号30の署名記録の情報が保存されている。
記録番号30の署名記録は、Bに文書を送信した時に生成したものである。

フロントページの続き

(72)発明者　宮崎　邦彦
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　大本　周広
東京都江東区新砂一丁目６番27号　株式会社日立製作所公共システム事業部内
(72)発明者　西岡　佳津子
東京都江東区新砂一丁目６番27号　株式会社日立製作所公共システム事業部内

Ｆターム(参考)　5J104 AA07 EA19 KA01 KA03 LA03 LA06 NA12 PA07 PA10